IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO

SHERYL JACKSON, on behalf of herself and all others similarly situated, Plaintiff, v. **NATIONWIDE RETIREMENT SOLUTIONS, INC.,** Defendant.	Case No. Judge **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Sheryl Jackson ("Plaintiff") brings this Class Action Complaint against Nationwide Retirement Solutions, Inc. ("Nationwide" or "Defendant"), as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions and her counsels' investigation, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant Nationwide Retirement Solutions, Inc., a Columbus, Ohio based pension and retirement planning company, to seek damages for herself and other similarly situated current and former customers ("customers"), or any other person(s) impacted in the data breach at issue ("Class Members") who she seeks to represent, as well as other equitable relief, including, without limitation, injunctive relief designed to protect the very sensitive information of Plaintiff and other Class Members. This action arises from Defendant's failure to properly secure and safeguard personal identifiable information, including without limitation, unencrypted and unredacted names, Social Security numbers, dates of birth, email addresses, phone numbers, and gender information (collectively, "PII").

2. Plaintiff alleges Nationwide failed to provide timely, accurate and adequate notice to Plaintiff and Class Members who were or are customers of Nationwide. Current and former customers' knowledge about what PII Nationwide lost, as well as precisely what types of

information was unencrypted and in the possession of unknown third parties, was unreasonably delayed by Nationwide's unreasonable notification delay after it first learned of the data breach.

3. On or about September 13, 2022, Nationwide notified state Attorneys General about a widespread data breach involving sensitive PII of thousands of individuals occurred. Nationwide explained in its required notice letter that it discovered an unauthorized third-party gained access to a portion of Nationwide's network. Nationwide discovered that files on its network were accessed and acquired by the unknown actor (the "Data Breach").

4. On September 3, 2022, Nationwide chose not to notify affected customers or, upon information and belief, anyone of its data breach instead choosing to address the incident in-house by implementing other safeguards to some aspects of its computer security.

5. On September 6, 2022, Nationwide concluded its investigation, but did not notify Class Members' that their PII had been impacted for over a week.[1]

6. Nationwide and its network service provider "immediately launched an investigation," and determined that Plaintiff's and Class Members' PII (including but not limited to full names, Social Security numbers, dates of birth, etc.) was present and potentially stolen by the unauthorized person at the time of the incident.[2]

7. Plaintiff and the Class Members in this action were, upon information and belief, current and former customers of Nationwide. Upon information and belief, the first that Plaintiff and the Class Members learned of the Data Breach was when they received by U.S. Mail Notice of Data Breach letters on September 13, 2022.

8. In its Notice Letters, sent to Plaintiff and Class Members, Nationwide failed to explain why it took the company a full week after confirming the breach occurred to alert Class Members that their sensitive PII had been exposed. As a result of this delayed response, Plaintiff and Class Members were unaware that their PII had been compromised, and that they were, and continue to be, at significant risk to identity theft and various other forms of personal, social, and

[1] https://media.dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-550.pdf
[2] *Id.*

financial harm.

9. Plaintiff's and Class Members' unencrypted, unredacted PII was compromised due to Nationwide's negligent and/or careless acts and omissions, and due to the utter failure to protect Class Members' sensitive data. Hackers obtained their PII because of its value in exploiting and stealing the identities of Plaintiff and similarly situated Class Members. The risks to these persons will remain for their respective lifetimes.

10. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Nationwide's failure to: (i) adequately protect Plaintiff and Class Member PII; (ii) warn Plaintiff and Class Members of its inadequate information security practices; and (iii) effectively monitor Nationwide's network for security vulnerabilities and incidents. Nationwide's conduct amounts to negligence and violates federal and state statutes.

11. Plaintiff and Class Members have suffered injury as a result of Nationwide's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (iv) the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges; change their usernames and passwords on their accounts; investigate, correct and resolve unauthorized debits; deal with spam messages and e-mails received subsequent to the Data Breach, (v) charges and fees associated with fraudulent charges on their accounts, and (vi) the continued and certainly an increased risk to their PII, which remains in Nationwide's possession and is subject to further unauthorized disclosures so long as Nationwide fails to undertake appropriate and adequate measures to protect the PII. These risks will remain for the lifetimes of Plaintiff and Class Members.

12. Nationwide disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or at the very least negligently failing to take and implement adequate and reasonable measures to ensure that its customer PII was safeguarded, failing to take available steps

to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As the result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

13. Plaintiff Sheryl Jackson is a resident and citizen of Florida, residing in Haines City. Ms. Jackson received Nationwide's notice of data breach correspondence, dated September 13, 2022, by U.S. Mail.

14. Defendant Nationwide Retirement Solutions, Inc., based in Columbus, Ohio, manages pension, retirement, health, and welfare funds for public sector employees. Nationwide has a principal place of business at 3400 Southpark Place, Suite A, Columbus, Ohio 43123.

15. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

16. All of Plaintiff's claims stated herein are asserted against Nationwide and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

17. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

18. The Southern District of Ohio has personal jurisdiction over Defendant named in this action because Defendant and/or its parents or affiliates are headquartered in this District and

Defendant conducts substantial business in Ohio and this District through its headquarters, offices, parents, and affiliates.

19. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

IV. FACTUAL ALLEGATIONS

Background

21. Defendant Nationwide Retirement Solutions, Inc. is a Columbus, Ohio company that manages pension, retirement, health, and welfare funds for public sector employees.

22. In its notice of data breach letters sent to Plaintiff Jackson and Class Members, Nationwide indicated that protecting the privacy of private information is a "top priority" to Nationwide, and Nationwide purports that it has taken the steps to prevent "this issue" from reoccurring.

21. Plaintiff and the Class Members, as current or former customers of Nationwide, reasonably relied (directly or indirectly) on this sophisticated company to keep their sensitive PII confidential; to maintain its system security; to use this information for business purposes only; and to make only authorized disclosures of their PII. Customers, in general, demand security to safeguard their PII, especially when financial information and other sensitive PII is involved.

22. Nationwide had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII from involuntary disclosure to third parties.

The Data Breach

23. On or around September 13, 2022, Nationwide first began notifying Class Members and state Attorneys General ("AGs") about a widespread data breach of its computer network involving the sensitive PII of persons.[3]

24. According to its notice letters to Class Members, Nationwide explained it

[3] *Id.*

discovered on September 3, 2022, that it detected an unauthorized third-party gained access to a portion of its computer network.

25. On or about September 13, 2022, Nationwide notified state Attorneys General about a widespread data breach involving sensitive PII of impacted individuals.

26. For nearly two weeks, Nationwide chose not to notify affected Class Members, or upon information and belief, anyone, of its data breach instead choosing to address the incident in-house by implementing other safeguards to some aspects of its computer security. It then simply resumed its normal business operations.

27. On September 13, 2022, Nationwide admitted that Class Members' PII had been impacted and taken from its network.

28. Nationwide immediately launched an investigation and determined that Plaintiff's and Class Members' PII (including but not limited to full names, Social Security numbers, dates of birth, addresses, etc.) was present and potentially stolen by the unauthorized person at the time of the incident.[4]

29. Plaintiff and Class Members in this action were, upon information and belief, current and former customers of Nationwide. The first that Plaintiff and Class Members learned of the Data Breach was when they received by U.S. Mail Notice of Data Breach letters dated September 13, 2022.

30. The confidential information that was accessed without authorization included persons' full names along with Social Security numbers, dates of birth, email addresses, phone numbers, and gender information.

31. Upon information and belief, the PII was not encrypted prior to the data breach.

32. Upon information and belief, the cyberattack was targeted at Nationwide as pension and retirement plan company that collects and maintains valuable personal, health, tax, and financial data from its current and former customers.

[4] *Id.*

33. Upon information and belief, the cyberattack was expressly designed to gain access to private and confidential data, including (among other things) the PII of Plaintiff and the Class Members.

34. Beginning on or about September 13, 2022, Nationwide sent affected persons (including Plaintiff Jackson) a written correspondence regarding the Data Breach, informing the recipients that their confidential data was involved.

35. Nationwide admitted in its written correspondence to the affected persons that their systems were subjected to unauthorized access in September 2022. Nationwide made no indication to either state Attorneys General or the Class Members that the exfiltrated PII was retrieved from the cybercriminals who took it. Nationwide admitted the information was acquired by the unauthorized party.

36. In response to the Data Breach, Nationwide claims it has further secured their systems to protect the private information. Nationwide admits additional security was required, but there is no indication whether these steps are adequate to protect Plaintiff's and Class Members' PII going forward.

37. Nationwide had obligations created by contract, industry standards, common law, and representations made to its customers and employees to keep the PII of Plaintiff and Class Members that was entrusted to Nationwide confidential, and to protect the PII from unauthorized access and disclosure.

38. Plaintiff and Class Members provided their PII to Nationwide with the reasonable expectation that Nationwide, as a sophisticated company, would comply with its duty and obligations and representations to keep such information confidential and secure from unauthorized access.

39. Nationwide failed to uphold its data security obligations to Plaintiff and Class Members. As a result, Plaintiff and Class Members are significantly harmed and will be at a high risk of identity theft and financial fraud for many years to come.

40. Nationwide did not use reasonable security procedures and practices appropriate to

the nature of the sensitive, unencrypted information it was maintaining, causing Plaintiff's and Class Members' PII to be exposed.

Securing PII and Preventing Breaches

41. Nationwide could have prevented this Data Breach by properly encrypting or otherwise protecting their equipment and computer files containing PII.

42. In its notice letters, Nationwide acknowledged the sensitive and confidential nature of the PII. To be sure, collection, maintaining, and protecting PII is vital to virtually all of Nationwide's business purposes. Nationwide acknowledged through its conduct and statements that the misuse or inadvertent disclosure of PII can pose major privacy and financial risks to impacted individuals, and that under state law they may not disclose and must take reasonable steps to protect PII from improper release or disclosure.

The Cyber Attack and Data Breach were Foreseeable Risks of which Defendant was on Notice

43. It is well known that PII, including financial account information in particular, is an invaluable commodity and a frequent target of hackers.

44. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[5]

45. Of the 1,473 recorded data breaches, 108 of them were in the banking/credit/financial industry, with the number of sensitive records being exposed exceeding 100 million. In fact, over 62% of the 164 million sensitive records exposed in data breaches in 2019 were exposed in those 108 breaches in the banking/credit/financial sector.[6]

46. The 108 reported financial sector data breaches reported in 2019 exposed 100,621,770 sensitive records, compared to 2018 in which only 1,778,658 sensitive records were exposed in financial sector breaches.[7]

---

[5] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed December 10, 2021)
[6] *Id.*
[7] *Id* at p. 15.

47. Individuals place a high value not only on their PII, but also on the privacy of that data. For the individual, identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.

48. Individuals are particularly concerned with protecting the privacy of their Social Security numbers, which are the "secret sauce" for hackers.

49. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Nationwide knew or should have known that its electronic records would be targeted by cybercriminals.

50. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

51. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite their own acknowledgment of its duties to keep PII private and secure, Nationwide failed to take appropriate steps to protect the PII of Plaintiff and the proposed Class from being compromised.

At All Relevant Times Nationwide Had a Duty to Plaintiff and Class Members to Properly Secure their PII

52. At all relevant times, Nationwide had a duty to Plaintiff and Class Members to properly secure their PII, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiff and Class Members, and to *promptly* notify Plaintiff and Class Members when Nationwide became aware that their PII may have been compromised.

53. Nationwide's duty to use reasonable security measures arose as a result of the special relationship that existed between Nationwide, on the one hand, and Plaintiff and the Class

Members, on the other hand. The special relationship arose because Plaintiff and the Members of the Class entrusted Nationwide with their PII when they were customers of Nationwide.

54. Nationwide had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, Nationwide breached its common law, statutory, and other duties owed to Plaintiff and Class Members.

55. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PII;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

56. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[8] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number,

[8] 17 C.F.R. § 248.201 (2013).

employer or taxpayer identification number."[9]

57. The ramifications of Nationwide's failure to keep its Class Members' PII secure are long lasting and severe. Once PII is stolen, particularly financial information, fraudulent use of that information and damage to victims is likely to continue for years.

The Value of Personal Identifiable Information

58. PII of data breach victims remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[10] According to the Dark Web Price Index for 2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120.[11]

59. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[12]

60. PII can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with

---

[9] *Id.*

[10] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed December 10, 2021).

[11] *Dark Web Price Index 2021*, Zachary Ignoffo, March 8, 2021, *available at*: https://www.privacyaffairs.com/dark-web-price-index-2021/ (last accessed December 10, 2021).

[12] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed December 10, 2021).

other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[13]

61. Given the nature of Nationwide's Data Breach, as well as the long delay in notification to Class Members, it is foreseeable that the compromised PII has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiff's and Class Members' PII may easily obtain Plaintiff's and Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

62. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, basic credit card information in a retailer data breach, because credit card victims can cancel or close credit and debit card accounts.[14] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as dates of birth).

63. To date, Nationwide has only offered its Class Members basic credit monitoring services even with the delay from their discovery of the Data Breach to the production of the notice letters. The advice offered to victims in the notice letters is inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

64. The injuries to Plaintiff and Class Members were directly and proximately caused by Nationwide's failure to implement or maintain adequate data security measures for the Class Members.

Nationwide Failed to Comply with FTC Guidelines

65. Federal and State governments have established security standards and issued recommendations to lessen the risk of data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for

[13] *See* OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1.
[14] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes, Mar 25, 2020, *available at*: https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last accessed December 10, 2021).

business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[15]

66. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[16] The guidelines note businesses should protect the personal consumer and consumer information that they keep, as well as properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

67. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[17]

68. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

---

[15] Federal Trade Commission, *Start With Security, available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed September 22, 2022).

[16] Federal Trade Commission, *Protecting Personal Information: A Guide for Business, available at*: https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last accessed September 22, 2022).

[17] FTC, *Start with Security*, *supra* note 34.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

69. The FTC has brought enforcement actions against businesses for failing to protect consumer and consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

70. Because Class Members entrusted Nationwide with their PII directly or indirectly through Nationwide, Nationwide had, and has, a duty to the Class Members to keep their PII secure.

71. Plaintiff and the other Class Members reasonably expected that when they provided PII to Nationwide, that Nationwide would safeguard their PII.

72. Nationwide was at all times fully aware of its obligation to protect the personal data of its customers, including Plaintiff and members of the Classes. Nationwide was also aware of the significant repercussions if it failed to do so.

73. Nationwide's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—including Plaintiff's and Class Members' full names, Social Security numbers, and other highly sensitive and confidential information—constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Plaintiff and Class Members Have Suffered Concrete Injury as a Result of Defendant's Inadequate Security and the Data Breach it Allowed.

74. Plaintiff and Class Members reasonably expected that Defendant would provide adequate security protections for their PII, and Class Members provided Defendant with sensitive personal information, including their private financial information.

75. Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendant for services, Plaintiff and other reasonable Class Members understood and expected that their PII would be protected with data security, when in fact Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected. As such, Plaintiff and the Class Members suffered pecuniary injury.

76. Cybercriminals capture PII to exploit it; the Class Members are now, and for the rest of their lives will be, at a heightened risk of identity theft. Plaintiff has also incurred (and will continue to incur) damages in the form of, *inter alia*, loss of privacy and costs of engaging adequate

credit monitoring and identity theft protection services.

77. The cybercriminals who obtained the Class Members' PII may exploit the information they obtained by selling the data in so-called "dark markets." Having obtained these names, contact information, financial information, and other PII, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class Member's name, including but not limited to:

a. obtaining employment;

b. obtaining a loan;

c. applying for credit cards or spending money;

d. filing false tax returns;

e. stealing Social Security and other government benefits; and

f. applying for a driver's license, birth certificate, or other public document.

78. In addition, if a Class Member's PII is used to create false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, impairing the person's ability to gain employment or obtain a loan.

79. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiff and the other Class Members have been deprived of the value of their PII, for which there is a well-established national and international market.

80. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.[18]

81. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and the other Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud.[19] Indeed, "[t]he level of risk is

[18] *Id.*

[19] *Data Breach Victims More Likely To Suffer Identity Fraud*, INSURANCE INFORMATION INSTITUTE BLOG (February 23, 2012), http://www.iii.org/insuranceindustryblog/?p=267 (last accessed December 10, 2021).

growing for anyone whose information is stolen in a data breach."[20] Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud."[21] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class Members' PII will do so at a later date or re-sell it.

82. As a result of the Data Breach, Plaintiff and Class Members have already suffered damages.

83. In its notice letter, Defendant represented to the Class Members and AGs that it initially discovered the Data Breach in September 2022, and admitted files were accessed and acquired by the cybercriminals. As EmiSoft, an award-winning malware-protection software company, states "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence, *especially during the preliminary stages of the investigation*."[22] It is likely that the cybercriminals did steal data and did so undetected.

84. In this case, according to Defendant's notification to the Class Members, cybercriminals had access to Class Members' data at least on September 3, 2022, its notice letters about that Data Breach did not go out until September 13, 2022. This is tantamount to the cybercriminals having a head start on stealing the identities of Plaintiff and Class Members.

85. Accordingly, that Defendant has not found evidence of data being viewed is not an assurance that the data were not accessed, acquired, and stolen. Indeed, the likelihood that

---

[20] Susan Ladika, *Study: Data Breaches Pose A Greater Risk*, CREDITCARDS.COM (July 23, 2014), https://www.susanladika.com/freelance_writer_susan_ladika_personal_finance_data_breaches_pose_a_greater_risk.html (last accessed September 22, 2022).

[21] THE CONSUMER DATA INSECURITY REPORT: EXAMINING THE DATA BREACH- IDENTITY FRAUD PARADIGM IN FOUR MAJOR METROPOLITAN AREAS, (*available at* https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf) (last accessed September 22, 2022).

[22] EmiSoft Malware Lab, *The chance of data being stolen in a ransomware attack is greater than one in ten* (EMISOFT BLOG July 13, 2020), https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/ (last accessed September 22, 2022, emphasis added)).

cybercriminals stole the data covertly is significant, likely, and concerning.

Plaintiff Sheryl Jackson's Experience

86. On or about September 13, 2022, Ms. Sheryl Jackson, a citizen and resident of Haines City, Florida received Notice of Data Security Incident Letter by US. Mail.

87. As a customer of Nationwide, she provided her PII to Nationwide as part of its pension and retirement services, and under state and federal law, she was required to do so. She reasonably relied on Nationwide, a sophisticated company, to protect the security of her PII.

88. As a result of the Data Breach and the information that she received in the notice letter, Ms. Jackson has spent hours dealing with the consequences of the Data Breach (changing passwords, and self-monitoring bank and credit accounts), as well as her time spent verifying the legitimacy of the written correspondence, communicating with her bank, exploring credit monitoring and identity theft insurance options, and signing up for the credit monitoring. This time has been lost forever and cannot be recaptured.

89. Ms. Jackson is very careful about sharing her own personal identifying information and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

90. Ms. Jackson stores any and all documents containing PII in a secure location and destroys any documents she receives in the mail that contain any PII or that may contain any information that could otherwise be used to compromise her identity and credit card accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

91. Ms. Jackson suffered actual injury and damages due to Nationwide's mismanagement of her PII before the Data Breach.

92. Ms. Jackson suffered actual injury in the form of damages and diminution in the value of her PII—a form of intangible property that she entrusted to Nationwide, which was compromised in and as a result of the Data Breach.

93. Ms. Jackson suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach, and she has suffered anxiety and increased concerns for the theft of her

privacy since she received the Notice Letter. She is especially concerned about the theft of her full name paired with her Social Security number.

94. Ms. Jackson has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her stolen PII, especially her social security number, being placed in the hands of unauthorized third parties and possibly criminals.

95. Ms. Jackson has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Nationwide's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

96. Plaintiff brings this nationwide class action on behalf of herself and on behalf of all others similarly situated.

97. The Class that Plaintiff seeks to represent is defined as follows:

> **All persons residing in the United States whose PII was compromised in the September 2022 data breach announced by Nationwide Retirement Solutions, Inc. (the "Class").**

98. Excluded from the Classes are the following individuals and/or entities: Nationwide Retirement Solutions, Inc., and Nationwide's parents, subsidiaries, affiliates, officers and directors, and any entity in which Nationwide has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

99. Plaintiff reserves the right to modify or amend the definition of the proposed class and any future subclass before the Court determines whether certification is appropriate.

100. Numerosity, Fed R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are thousands of individuals

whose PII may have been improperly accessed in the Data Breach, and each Class is apparently identifiable within Defendant's records.

101. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Class exists and predominates over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect Plaintiff's and Class Members' PII;

b. Whether Defendant had duties not to disclose the Plaintiff's and Class Members' PII to unauthorized third parties;

c. Whether Defendant had duties not to use Plaintiff's and Class Members' PII for non-business purposes;

d. Whether Defendant failed to adequately safeguard Plaintiff's and Class Members' PII;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' PII;

k. Whether Defendant violated the consumer protection statutes invoked herein;

l. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or

nominal damages as a result of Defendant's wrongful conduct;

m. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

n. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

102. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

103. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

104. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intend to prosecute this action vigorously.

105. Predominance, Fed. R. Civ. P. 23(b)(3): Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single

action has important and desirable advantages of judicial economy.

106. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

107. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

108. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

109. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

110. Unless a Class-wide injunction is issued, Defendant may continue in their failure to properly secure and unlawful disclosure of the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

111. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

112. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;
b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;
c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
d. Whether a contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that contract;
e. Whether Defendant breached the contract;
f. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;
g. Whether Defendant breached the implied contract;
h. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their PII had been compromised;
i. Whether Defendant failed to implement and maintain reasonable security

procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' PII;

k. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

FIRST COUNT
Negligence
(On Behalf of Plaintiff and the Class)

113. Plaintiff restates and reallege all of the foregoing paragraphs as if fully set forth herein.

114. As a condition of being a customer of Nationwide, current and former customers are obligated to provide Nationwide with certain PII, including but not limited to, their names, Social Security numbers, dates of birth, email addresses, phone numbers, and gender information.

115. Plaintiff and Class Members entrusted their PII to Nationwide on the premise and with the understanding that Nationwide would safeguard their information, use their PII for legitimate business purposes only, and/or not disclose their PII to unauthorized third parties.

116. Nationwide has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

117. Nationwide knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII involved an unreasonable risk of harm to Plaintiff and Class Members, even if the harm occurred through the criminal acts of a third party.

118. Nationwide had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Nationwide's security protocols to ensure that Plaintiff's and Class Members' information in Nationwide's possession was adequately secured and protected.

119. Nationwide also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class Members' PII.

120. A breach of security, unauthorized access, and resulting injury to Plaintiff and Class Members was reasonably foreseeable, particularly in light of Nationwide's business as sophisticated life insurance company, for which the diligent protection of PII is a continuous forefront issue.

121. Plaintiff and Class Members were the foreseeable and probable victims of Nationwide's inadequate security practices and procedures. Nationwide knew of should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Nationwide's systems.

122. Nationwide's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Nationwide's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Nationwide's misconduct also included its decisions not to comply with industry standards for the safekeeping of Plaintiff's and Class Members' PII, including basic encryption techniques freely available to Nationwide.

123. Plaintiff and Class Members had no ability to protect their PII that was in, and possibly remains in, Nationwide's possession.

124. Nationwide was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

125. Nationwide had and continues to have a duty to adequately and promptly disclose that the PII of Plaintiff and Class Members within Nationwide's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

126. Nationwide had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and Class Members.

127. Nationwide has admitted that the PII of Plaintiff and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

128. Nationwide, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and Class Members during the time the PII was within Nationwide's possession or control.

129. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

130. These foregoing frameworks are existing and applicable industry standards in the financial services industry, and Defendant failed to comply with these accepted standards thereby opening the door to the cyber incident and causing the data breach.

131. Nationwide improperly and inadequately safeguarded the PII of Plaintiff and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

132. Nationwide failed to heed industry warnings and alerts to provide adequate safeguards to protect customer and employee PII in the face of increased risk of theft.

133. Nationwide, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of the PII.

134. Nationwide, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and Class Members the existence and scope of the Data Breach.

135. But for Nationwide's wrongful and negligent breach of duties owed to Plaintiff and

Class Members, the PII of Plaintiff and Class Members would not have been compromised.

136. There is a close causal connection between Nationwide's failure to implement security measures to protect the PII of Plaintiff and Class Members and the harm suffered or risk of imminent harm suffered by Plaintiff and Class. Plaintiff's and Class Members' PII was lost and accessed as the proximate result of Nationwide's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

137. As a direct and proximate result of Nationwide's negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Nationwide's possession and is subject to further unauthorized disclosures so long as Nationwide fails to undertake appropriate and adequate measures to protect the PII in their continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (ix) the diminished value of Nationwide's goods and services they received.

138. As a direct and proximate result of Nationwide's negligence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

139. Additionally, as a direct and proximate result of Nationwide's negligence, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII,

which remains in Nationwide's possession and is subject to further unauthorized disclosures so long as Nationwide fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

SECOND COUNT
Intrusion Upon Seclusion / Invasion of Privacy
(On Behalf of Plaintiff and the Class)

140. Plaintiff restates and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

141. Plaintiff and Class Members had a reasonable expectation of privacy in the PII Defendant mishandled.

142. Defendant's conduct as alleged above intruded upon Plaintiff's and Class Members' seclusion and privacy under common law.

143. Defendant invaded Plaintiff's and Class Members' right to privacy and intruded into Plaintiff's and Class Members' private life by intentionally misusing and/or disclosing their PII without their informed, voluntary, affirmative, and clear consent.

144. The PII disclosed by Defendant has no legitimate reason to be known by the public.

145. Defendant intentionally concealed from Plaintiff and Class Members an incident that misused and/or disclosed their PII without their informed, voluntary, affirmative, and clear consent.

146. Defendant acted with reckless disregard for the privacy of Plaintiff and Class Members rising to the level of (1) an intentional intrusion by Defendant, (2) into a matter that Plaintiff and Class Members have a right to keep private (i.e., their PII), and (3) which is highly offensive to a reasonable person.

147. Such an intrusion into Plaintiff's private affairs is likely to cause outrage, shame, and mental suffering because the information disclosed is typically only shared with others when

an individual is comfortable.

148. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it had actual knowledge that its information security practices were inadequate and insufficient. For example, Defendant knew that PII was stored for years after Defendant no longer had a legitimate use for such data. Defendant also knew that the PII it stored was not securely encrypted, and that its systems were vulnerable to foreseeable threats as a result of inadequate security measures and training.

149. Moreover, upon information and belief, the Data Breach was the result of a phishing attack, which both Defendant's security software and Defendant's employees should have recognized, as this is the most common method of effectuating a data breach.[23] By revealing necessary credentials to access the system or network storing Plaintiff's and Class Members' PII in response to a phishing attack, Defendant actively disclosed Plaintiff's and Class Members' PII and invaded their privacy.

150. Defendant acted with such reckless disregard as to the safety of Plaintiff's and Class Members' PII to rise to the level of intentionally allowing the intrusion upon Plaintiff's and Class Members' seclusion.

151. Plaintiff and Class Members have been damaged by the invasion of their privacy in an amount to be determined at trial.

---

[23] *See* https://en.wikipedia.org/wiki/Phishing ("As of 2020, phishing is by far the most common attack performed by cybercriminals, the FBI's Internet Crime Complaint Centre recording over twice as many incidents of phishing than any other type of computer crime.") (citing *Internet Crime Report 2020*, FBI Internet Crime Complaint Centre. U.S. Federal Bureau of Investigation. Retrieved 21 March 2021); *see also* https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/ (last visited Sept. 16, 2022) ("Phishing is the most common type of social engineering, which is a general term describing attempts to manipulate or trick computer users. Social engineering is an increasingly common threat vector used in almost all security incidents. Social engineering attacks, like phishing, are often combined with other threats, such as malware, code injection, and network attacks.").

THIRD COUNT
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

152. Plaintiff restates and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

153. When Plaintiff and Class Members provided their PII to Nationwide in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

154. Defendant solicited and invited Class Members to provide their PII as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

155. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

156. Class Members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

157. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

158. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

159. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their PII.

160. As a direct and proximate result of Defendant's breaches of the implied contracts, Class Members sustained damages as alleged herein.

161. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

162. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

FOURTH COUNT
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

163. Plaintiff restates and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

164. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became guardians of Plaintiff's and Class Members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for the benefit of its customers, including Plaintiff and Class Members, as follows: (1) for the safeguarding of Plaintiff's and Class Members' PII; (2) to timely notify Plaintiff and Class Members of a data breach and disclosure; and (3) to maintain complete and accurate records of what customer information (and where) Defendant did and does store.

165. Defendant had a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of this relationship, in particular, to keep secure the PII of its

customers.

166. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

167. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' PII.

168. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

169. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to ensure the confidentiality and integrity of electronic PII Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1).

170. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic PII to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1).

171. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1).

172. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to identify and respond to suspected or known security incidents and to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii).

173. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PII in violation of 45 C.F.R. § 164.306(a)(2).

174. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' PII.

175. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

176. As a direct and proximate result of Defendant's breaching its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

FIFTH COUNT
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

177. Plaintiff restates and re-alleges each and every allegation contained in the Complaint as if fully set forth herein.

178. This count is plead in the alternative to Count 4 (breach of implied contract).

179. Plaintiff and Class Members conferred a monetary benefit on Defendant, by paying Defendant money for retirement and pension services, a portion of which was to have been used for data security measures to secure Plaintiff's and Class Members' PII, and by providing Defendant with their valuable PII.

180. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

181. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

182. Defendant acquired the monetary benefit and PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

183. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

184. Plaintiff and Class Members have no adequate remedy at law.

185. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

186. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

187. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all Class Members, requests judgment against Nationwide Retirement Solutions, Inc. and that the Court grant the following:

A. For an Order certifying the Nationwide Classes and appointing Plaintiff and her

Counsel to represent the certified Class;

B. For equitable relief enjoining Nationwide from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class Members' PII, and from refusing to issue prompt, complete, any accurate disclosures to the Plaintiff and Class;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the Class, including but not limited to an order:

i. prohibiting Nationwide from engaging in the wrongful and unlawful acts described herein;

ii. requiring Nationwide to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Nationwide to delete, destroy, and purge the personal identifying information of Plaintiff and Class unless Nationwide can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and the Class;

iv. requiring Nationwide to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff's and Class Members' personal identifying information;

v. prohibiting Nationwide from maintaining Plaintiff's and Class Members' personal identifying information on a cloud-based database;

vi. requiring Nationwide to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Nationwide's systems on a periodic basis, and ordering Nationwide to promptly

correct any problems or issues detected by such third-party security auditors;

vii. requiring Nationwide to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Nationwide to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Nationwide to segment data by, among other things, creating firewalls and access controls so that if one area of Nationwide's network is compromised, hackers cannot gain access to other portions of Nationwide's systems;

x. requiring Nationwide to conduct regular database scanning and securing checks;

xi. requiring Nationwide to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Nationwide to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Nationwide to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Nationwide's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Nationwide to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor

Nationwide's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Nationwide to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Nationwide to implement logging and monitoring programs sufficient to track traffic to and from Nationwide's servers; and

xvii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Nationwide's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of punitive damages;

F. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. For prejudgment interest on all amounts awarded; and

H. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: September 27, 2022

Respectfully Submitted,

/s/ Terence R. Coates
Terence R. Coates (0085579)
Justin C. Walker (0080001)
Jonathan T. Deters (0093976)
Dylan J. Gould (0097954)

MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
jwalker@msdlegal.com
jdeters@msdlegal.com
dgould@msdlegal.com

Attorneys for Plaintiff and the Proposed Class